

Data Processing Agreement: Zenshin Kaishi organization scan

VERSION 1.1 · 26 OCTOBER 2026

In plain words

- This is the contract between Zenshin Kaishi and an organization that runs a scan.
 - The organization decides the scan happens and who is invited.
 - So the organization is responsible for the data, and we work for it.
 - The law calls the organization the controller, and us the processor.
 - We use the data only for the scan, and only as the organization instructs.
 - We keep it safe, in the European Union, and list who else handles it.
 - A data leak reaches the organization within 48 hours.
 - Our liability is capped at the price of the scan concerned.
 - Some results can point to one person, and the contract lists each case.
 - After an account closes, its answers stay, no longer linked to the person.
 - Every clause says what the service does, including its limits.
-

Parties

(1) **Plakboom B.V.**, registered in the Netherlands under Chamber of Commerce (KVK) number 34130965, VAT number NL808917444B01, with its seat at Lanckhorstlaan 115, 2101 BC Heemstede, the Netherlands, operating the service under the name **Zenshin Kaishi** ("Zenshin Kaishi"); and

(2) _____, registered under number _____, with its seat at _____ (the "Organization").

Background

A. The Organization has commissioned an innovation–culture scan. People associated with the Organization are invited to answer questions: its leaders, managers and employees and, if the Organization chooses, its partners and customers. The Organization receives a report built from group results.

B. In running that scan, Zenshin Kaishi processes personal data on the Organization's behalf. This Agreement governs that processing and is the contract required by Article 28(3) GDPR.

C. Zenshin Kaishi also processes some personal data for its own purposes, not on the Organization's instructions. Part B sets these out, and Zenshin Kaishi is the controller for them.

Part A: Zenshin Kaishi as processor

1. Definitions

1.1 "GDPR" means Regulation (EU) 2016/679. "Controller", "processor", "personal data", "processing", "data subject", "personal data breach" and "supervisory authority" have the meanings given in it.

1.2 "Respondent" means a natural person invited by the Organization to answer a scan.

1.3 "Round" means one measurement cycle commissioned by the Organization, from the moment it opens to the moment it closes.

1.4 "Service" means the Zenshin Kaishi organization scan as provided to the Organization.

1.5 "Administrator" means a person to whom the Organization has given the owner, admin or analyst role in the Service (Annex 2, section 5).

1.6 "Minimum" means the number of employees in a group who must have answered before that group's result is shown (clause 5.4(a)).

2. Roles and scope

2.1 For the processing described in Annex 1, the Organization is the controller and Zenshin Kaishi is the processor. The Organization decides that the Round happens, who is invited and in which group, when it opens and closes, and the settings in clause

5.4. Those decisions determine the purposes of the processing, and the purposes are the Organization's.

2.2 This Agreement applies from the date it is signed and continues for as long as Zenshin Kaishi processes personal data on the Organization's behalf. It forms part of the Zenshin Kaishi terms of service (clause 11.1 of those terms) and, on any matter of personal data processing, prevails over them.

2.3 For the processing in Part B, Zenshin Kaishi is the controller, not the processor. Nothing in Part A makes the Organization responsible for it.

3. Instructions: Art. 28(3)(a)

3.1 Zenshin Kaishi processes personal data only on the Organization's documented instructions, including as to transfers to a third country, unless required to do otherwise by Union or Member State law. In that case it informs the Organization of the requirement before processing, unless that law prohibits this on important grounds of public interest. Clause 9.2 states the one processing that continues after an account closes, and Part B.1(c) the purpose it serves.

3.2 The instructions are this Agreement, the configuration the Organization sets in the Service, and any further written instruction the Parties agree. Configuration covers who is invited, the group each person is invited as, when the Round opens and closes, the settings in clause 5.4, the optional note to the people invited (clause 13.6), and whether partners and customers receive a letter when the Round closes (clause 13.7).

3.3 If Zenshin Kaishi considers that an instruction infringes the GDPR or other Union or Member State data protection law, it immediately tells the Organization. It may suspend the affected processing until the instruction is withdrawn or confirmed.

3.4 A Round bought online opens only once it is paid for. A Round bought on a quote can open before it is paid. Until a Round opens, nobody can be invited to it. The number of people invited to a Round cannot exceed the number of people paid for. Each address counts once. A withdrawn invitation gives its place back, unless the person had already accepted it.

4. Confidentiality: Art. 28(3)(b)

4.1 Zenshin Kaishi ensures that the persons it authorises to process the personal data are bound by an obligation of confidentiality, and that each has only the access needed to run and support the Service.

5. Security: Art. 28(3)(c), Art. 32

5.1 Zenshin Kaishi implements the technical and organizational measures set out in **Annex 2**, having regard to the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the risk to the rights and freedoms of natural persons.

5.2 The measures in Annex 2 are the ones actually in force. Zenshin Kaishi may change the measures, but not in a way that lowers the level of protection.

5.3 The central measure is architectural. Identity is discarded at a one-way aggregation boundary, so the Organization's report consists of group results with no key back to an individual. Five things reach the Organization beyond that. Each is stated here so none is discovered later:

(a) **participation information**: the address and role of each person invited, and counts per role of how many people accepted, declined, started and finished (clause 13.5);

(b) **results not held to the Minimum**: leaders' and managers' results from one person, and partners' and customers' results at any group size (clause 5.5(a));

(c) **employees' written remarks**, without names, with the writer's consent (clause 5.5(b));

(d) **leader quotes** and **interview mode**, each switched on by the leader concerned (clauses 5.4(b) and 5.5(c)); and

(e) **a team lead's shared answers**, in a team scan, shared by the lead (clause 5.5(d)).

5.4 Two settings are the Organization's to choose. They are named here so that each choice, and its consequence, rests with the Party that makes it:

(a) **A lower Minimum for employees**. By default, an employee group's result is shown only when at least five employees in that group have answered. In scans of up to 20 people, the Minimum is three by default. A scan's size is the largest of three numbers: the people it declares will take part, the places bought for it, and the people invited to it. The Minimum applies to all of the Organization's scans, so its largest scan counts. The Minimum of three is set when the Organization saves the size of a scan of up to 20 people, before anyone in the Organization has answered. The moment it is set is recorded. Set-up shows the Organization the disclosure that individual answers may be recognizable to colleagues. Each employee affected must then acknowledge the same fact on their own scan before their first question, and can stop there. The Minimum protects employees only. It

does not apply to leaders, managers, partners or customers (clause 5.5(a)). An employee group below it is not shown on its own, and the report shows no count from which that group's size could be worked out. Its answers still count in the Organization's scores. The 20-person limit is checked again whenever a scan's declared size, the places bought for it or the people invited to it grow. Once any of the Organization's scans holds more than 20 people, the Minimum returns to five, and the Service tells the people running the scan. The Organization can restore the Minimum of five at any time.

(b) Leader naming. The Organization may offer its leaders the option to go on the record. Where a scan has leaders but no managers, the Organization must offer it, because otherwise that scan has no authority side for its patterns to conclude on. Each leader then decides for themselves, for their own scan, by accepting a disclosure. If a leader accepts, their written answers to certain questions may be quoted in the Organization's report. Quotes are shown under the role "Leadership", never under the leader's name. Given their position, the leader will be recognizable, and the disclosure says so. If a leader does not accept, their written answers are not shown. Answers that could name a third party, and answers about the leader's own working life, are never quoted. The disclosure is shown before the first question, but answering does not wait for it. A leader can accept it only before their first answer is saved. The Service has no button to withdraw an acceptance. A leader withdraws it by writing to privacy@zenshinkaishi.com. The withdrawal applies to every result calculated afterwards, and clause 7.4 applies to results already calculated.

5.5 Four further exceptions are not the Organization's settings. They are properties of the Service, or choices of the Respondent concerned:

(a) Results not held to the Minimum. Leaders and managers answer in their professional capacity. Their results show per role from a single person: the Leadership Diagnostic, the Management Scan, and the items asked only of team leaders. They are told so in their invitation. Their answers about their own working life are the exception: these are treated as employee answers, shown only from five people, and left out of the role's scores. Partners and customers are shown at any group size, as two separate groups, without names. They are told so in their invitation. Their results never count towards the Organization's culture score, and their written answers are never shown to the Organization.

(b) Unattributed remarks. Some employee questions invite an optional answer in the Respondent's own words. Before any such question, the Respondent is shown a disclosure. If they decline, the question is not asked. If they answer, the owners,

admins and analysts can read the words verbatim, without a name, without a link to any other answer, sorted alphabetically rather than by arrival. Remarks are shown only once at least as many employees as the Minimum have written one.

(c) Interview (facilitation) mode. A leader may choose to take their scan as an interview. Someone who runs the scan for the Organization (an owner or admin) then asks the questions, types the leader's answers, and may note what the leader says about each answer. Only the leader can switch this on, by accepting a disclosure on their own scan. The interviewer can open and change the leader's answers only while that scan is open. The leader can read the notes.

(d) A team lead's shared answers. In a team scan, the lead sees their own answers to the statements about their working life beside the team's answers, privately. The team's side shows only where it clears the Minimum. Once the scan has closed, the lead may choose to share that comparison, with remarks of their own. Only the lead can share it, and the lead can withdraw the share, which deletes it. Once shared, the team members who finished the scan and the Organization's owners, admins and analysts see the lead's answers beside the team's.

Routes (c) and (d) are the only ones by which anyone on the Organization's side reads a named person's answers. Each is opened by the person whose answers they are.

6. Sub-processors: Art. 28(2), 28(4)

6.1 The Organization gives a general authorization for the sub-processors listed in **Annex 3: Cloudflare and Microsoft**. The page <https://zenshinkaishi.com/who-sees-what/sub-processors> lists them for data subjects. That page also names Stripe, which takes payments for Zenshin Kaishi. Under this Agreement Stripe is not a sub-processor of the Organization's scan, for the reasons in Annex 3.

6.2 Zenshin Kaishi gives the Organization at least 30 days' written notice before adding or replacing a sub-processor, at the address in clause 12.5. The Organization may object on reasonable data protection grounds within that period. If the objection cannot be resolved, the Organization may terminate the Service for the affected Round and is refunded the unused portion of what it paid.

6.3 Each sub-processor is bound by its own data processing terms with Zenshin Kaishi, named in Annex 3. Zenshin Kaishi is liable to the Organization for each sub-processor to the same extent as for itself, within the cap in clause 14.1.

7. Data subject rights: Art. 28(3)(e)

7.1 Taking into account the nature of the processing, Zenshin Kaishi assists the Organization, by appropriate technical and organizational measures, in responding to requests under Chapter III GDPR.

7.2 In practice, a Respondent with an account exercises most of these rights in the Service itself, without going through either Party. A signed-in Respondent can export everything linked to their account, and can delete their account. Deleting the account deletes their personal details and their written answers. Their coded answers stay, no longer linked to them, as clause 9.2 describes. An invited person can say no to an invitation from the link, without signing in. When a request comes through the Organization instead, Zenshin Kaishi tells the Organization what it can and cannot reach.

7.3 Where a Respondent's request concerns processing carried out on the Organization's behalf, Zenshin Kaishi does not respond to it directly, other than to point the Respondent to the self-service route or to the Organization. It forwards the request to the Organization without undue delay.

7.4 The following limits are properties of the architecture rather than of policy. The first three are shown to the Respondent when they delete their account:

- (a) a report already issued is not rewritten;

- (b) coded answers kept under clause 9.2 keep counting in the Organization's results. Where the Organization declined benchmarking, they are deleted instead, and they leave its results at the next recalculation, not a report already delivered;

- (c) a scan of the Respondent's own that they brought into the Round (clause 9.6) leaves the Organization's results at the next recalculation, because the permission they gave is deleted with their account; and

- (d) **stored report snapshots.** Each recalculation stores a new snapshot of the Organization's results beside the earlier ones. Nothing deletes earlier snapshots, and deletion and export do not reach them. Most of a snapshot is distributions with no identity. Two parts are words: quoted leader answers under 5.4(b) and unattributed remarks under 5.5(b). Both are stored encrypted. A leader who deletes their account, or withdraws their acceptance, drops out of the next snapshot, but stays in the earlier ones. So (b) and (c) are true of what is shown, not of what is stored.

- (e) **Invitees who never create an account.** Such a person cannot use the self-service routes, because there is no account to sign in to. A request about their

invitation record is handled by email to privacy@zenshinkaishi.com. When the Organization withdraws an invitation that was never accepted, the record keeps only a one-way fingerprint of the address, not the address itself. Invitations that never became an account (never accepted, declined, or withdrawn, fingerprints included) are deleted once their Round has been closed for 24 months. Before deleting them, the Service records how many people were invited to the Round, so its size does not change.

8. Assistance: Art. 28(3)(f)

8.1 Zenshin Kaishi assists the Organization in complying with Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to it.

8.2 This includes the information the Organization needs for a data protection impact assessment of the scan. Whether a DPIA is required is for the Organization to assess, as controller. Zenshin Kaishi provides the facts the Organization needs for one on request.

8.3 Personal data breaches are dealt with in clause 12.

9. Retention and deletion: Art. 28(3)(g)

9.1 **Retention runs per account.** Personal data processed under Part A is kept while the account it belongs to is in use. After 24 months without activity on an account, Zenshin Kaishi writes to the account holder or, for an account the Organization manages, to its Administrator. Signing in within 30 days keeps the account. Otherwise the account closes on the date in the letter. The Service has no clock per Organization or per Round. The Organization gives this instruction by entering into this Agreement.

9.2 **What happens when an account closes.** The same happens when the account holder deletes the account (clause 7.2). The person's identity, consent and disclosure records, interview notes, invitations, shared team-lead answers and any note they wrote to the people invited are deleted. Their written answers are deleted. Their coded answers (scales, choices, rankings) are kept, no longer linked to them. The kept answers still carry the Organization and the Round they belong to, so they are unlinked, not anonymous. Where the Organization declined benchmarking (clause 13.3), the coded answers are deleted as well. Where it agreed, or never answered the question, they are kept, so that one person's closed account does not take a result off a report the Organization paid for. The privacy notice says the same. Part B.1(c) states the purpose for which the kept answers are used.

9.3 Benchmarking. No benchmark exists today, and nothing is contributed to one. The Organization's answer to the benchmarking question is recorded before the Round opens (clause 13.3). Its effect today is the one in clause 9.2. Zenshin Kaishi updates this Agreement before any benchmark use begins.

9.4 The Organization's right to instruct otherwise. At any time, and when the Service ends, the Organization may instruct Zenshin Kaishi to delete or return all personal data processed on its behalf. Zenshin Kaishi carries out the instruction within 30 days, and confirms in writing when it is done. The instruction overrides clause 9.1 and reaches the unlinked answers in clause 9.2 and the stored snapshots in clause 7.4(d), because both still carry the Organization.

9.5 Two things are excepted from clause 9.4, and both are stated here rather than left to be discovered:

(a) **Records of the declarations** the Organization's Administrator made for a Round: who answered which question, when, the statement chosen, and the version of the wording (clause 13.3). These are kept as evidence that the step was taken, and are deleted five years after the Round closes. They are kept even after the declaring person's other data is deleted, together with the account record they name.

(b) **Statutory retention**, including the seven-year retention duty under Dutch tax law (Article 52 AWR) for invoices and related records.

9.6 An individual scan brought into a Round. A person who took a scan in their own right may, when invited, choose to bring their finished answers into the Organization's Round rather than answer again. From that moment, the copy that enters the Round is governed by clause 9.1. The person's original scan remains theirs and is governed by Part B. The person can withdraw that choice. Deleting their account deletes the permission, and clause 7.4(c) applies.

10. Audit: Art. 28(3)(h)

10.1 Zenshin Kaishi makes available to the Organization all information necessary to demonstrate compliance with Article 28. It allows for and contributes to audits, including inspections, conducted by the Organization or by an auditor it mandates.

10.2 In the ordinary case, documentation satisfies this: this Agreement's annexes, the published privacy notice, the works council briefing, and written answers to the Organization's questions within 30 days.

10.3 Beyond that, the Organization may conduct one audit per calendar year, on 30 days' written notice, during business hours, without unreasonable disruption, subject

to confidentiality, and at its own cost. If the audit reveals a material breach of this Agreement, Zenshin Kaishi bears the reasonable cost.

11. Transfers

11.1 The database in which personal data is stored was created with a setting that restricts it to the European Union, and replication to other regions is switched off.

11.2 The Service runs on a distributed edge network, so a request is handled at the network location nearest to the person sending it. A Respondent outside the EU, for example when travelling, sends their request directly. That is not a transfer by Zenshin Kaishi. Answers and accounts are stored in the EU. Cloudflare keeps a technical log of each request for 7 days. EU standard contractual clauses cover Cloudflare's request logs wherever they are stored.

11.3 Anything Cloudflare moves outside the EU runs under its processing agreement and the EU–US Data Privacy Framework, with the Standard Contractual Clauses as fallback.

11.4 Where any other sub-processor processes personal data outside the EEA, the transfer is covered by the Standard Contractual Clauses or another Article 46 mechanism, as recorded in Annex 3.

12. Personal data breach

12.1 Zenshin Kaishi notifies the Organization without undue delay, and in any event **within 48 hours** of becoming aware of a personal data breach affecting personal data processed on the Organization's behalf, or within any shorter period required by the Autoriteit Persoonsgegevens or another competent supervisory authority.

12.2 The window is 48 hours because the Organization must notify the Autoriteit Persoonsgegevens within 72 hours of becoming aware (Article 33(1) GDPR), and it is treated as aware once Zenshin Kaishi has told it. Forty-eight hours leaves the Organization twenty-four to decide and to file. Zenshin Kaishi does not wait for a complete picture before notifying.

12.3 The notification describes, as far as known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a point of contact. It is updated as more becomes known, not held back until complete.

12.4 Whether to notify a supervisory authority or the data subjects is the Organization's decision. Zenshin Kaishi does not make it on the Organization's behalf, and provides what the Organization needs to make it.

12.5 Notices under this clause go to the security contact the Organization names at signature, _____, and to privacy@zenshinkaishi.com.

12.6 Zenshin Kaishi handles a breach by a written procedure.

13. The Organization's own obligations

13.1 The Organization warrants that it has a lawful basis for the processing it instructs, and that it has given the Respondents the information required by Articles 13 and 14, to the extent Zenshin Kaishi's own privacy notice does not give it.

13.2 The Organization is responsible for the accuracy of the invitation list it supplies, and for making sure the people on it are the people it means to invite.

13.3 **Declarations, and employee representation.** Before a Round opens, the Service asks the Organization's Administrator up to four questions and records each answer: the statement chosen, who chose it, when, and the version of the wording. Answers can be given or changed only while the Round is a draft. Zenshin Kaishi records the answers and does not verify them.

(a) **Works council (required).** Where the Organization has a works council or equivalent body with a right to consent to, or be consulted on, employee surveys (for a Dutch works council, Article 27 of the Wet op de ondernemingsraden), the Organization is responsible for obtaining that consent or holding that consultation. The Organization decides which of the two applies. It answers with one of three statements: "We consulted our works council about this scan, or got its consent.", "We have no works council." or "Not yet." The Round cannot open while "Not yet." is the answer on record, and the Organization can answer again while the Round is a draft. Recording an answer is not an opinion by Zenshin Kaishi that a consultation was adequate or that a right applied.

(b) **Benchmarking (optional).** Whether combined results from this scan may be included in future benchmarks across organizations of similar size, industry or country. Its effect today is in clause 9.2.

(c) **Testimonial (optional).** Whether Zenshin Kaishi may name the Organization publicly as having used the method.

(d) **Letter to partners and customers (optional, asked only when they take part).** See clause 13.7.

13.4 The Organization acknowledges that the choices in clause 5.4 are its own, that it makes them against the disclosures shown at the moment of choosing, and that the same disclosures are shown to the Respondents.

13.5 Participation. The Organization's owners and admins can see the address of each person invited and the role they were invited for. Beyond that, participation is shown only as counts per role. Owners and admins see how many people accepted, are still pending, declined or were withdrawn. Owners, admins and analysts see how many people joined, started and finished. The counts never say which person did what. An employee count above zero and below the Minimum is shown as "fewer than" the Minimum. Leaders', managers', partners' and customers' counts are exact from one person, as their results are. The Organization undertakes not to use this to pressure an individual into answering, or to draw any conclusion about a person from whether they answered.

13.6 The note to the people invited. The person setting up a Round may write one optional note, in plain text, of at most 300 characters. It is shown, with the writer's name (or, without a name, their email address), in every invitation and in the letter that tells participants the results are open. The note is kept with the Round. It is deleted when the writer's account is deleted or closed.

13.7 The letter to partners and customers. Only if the Organization asks for it, by the declaration in clause 13.3(d), Zenshin Kaishi sends each partner and customer who finished the scan one letter when the Round closes. The letter is built from that person's own answers only, and names none of the Organization's results. The Organization receives no copy. Without that request, partners and customers receive nothing after they finish.

14. Liability, term and law

14.1 Liability. Zenshin Kaishi's liability under or in connection with this Agreement is capped at the price the Organization paid for the scan concerned. Zenshin Kaishi is not liable for indirect loss, such as lost profit.

14.2 Clause 14.1 does not apply to damage caused by intent or conscious recklessness (*opzet of bewuste roekeloosheid*). The law would not allow a cap there anyway. Nor does it limit a processor's liability to a data subject under Article 82(2) GDPR, or administrative fines under Article 83 GDPR.

14.3 This Agreement ends when the last processing under Part A ends and the obligations in clause 9 have been met. Clauses 4, 9.5, 10, 12 and 14 survive.

14.4 This Agreement is governed by Dutch law. Disputes are submitted to the competent court in Haarlem (Rechtbank Noord-Holland), the Netherlands.

Part B: Zenshin Kaishi as controller

A processor that determines the purposes of a processing operation is a controller for it (Art. 28(10)). This Part sets out where that is the case.

B.1 Zenshin Kaishi is the controller for:

(a) **Accounts and sign-in.** A Respondent's email address, and the sign-in record that lets them reach their own results.

(b) **The Respondent's own report, and how long it is kept.** A Respondent's relationship with Zenshin Kaishi over their own results exists whether or not their employer commissions anything. A scan taken in a person's own right follows the same clock as clause 9.1: after 24 months without activity Zenshin Kaishi writes to the person, signing in within 30 days keeps the account, and otherwise the account closes on the date in the letter. Personal details and written answers are then deleted, and coded answers are kept, no longer linked to the person. Deleting the account has the same result.

(c) **Answers kept after an account closes.** The coded answers kept under clause 9.2 and B.1(b), used to learn from and improve the method, and possibly for benchmarking in the future. No benchmark exists today. If one is built, it would compare combined results across organizations of similar size, industry or country, with no individual answer and no organization name. For that grouping, the Organization gives its size band at setup, and may give its industry and country. Answers from an Organization that declined benchmarking are not kept.

(d) **Records of the Organization's declarations** (clauses 9.5(a) and 13.3). These evidence Zenshin Kaishi's own compliance step, not the Organization's.

(e) **Billing.** The purchasing Administrator's email address, the billing name and address, and any VAT number, held with the payment provider (Annex 3). Also Zenshin Kaishi's own tax records of the sale, and the invoice references and numbers of people paid for that it records against a Round. Counting the people invited to a Round for invoicing is Zenshin Kaishi's own billing purpose. Checking that the Organization stays within the places it bought is done for the Organization, under Part A.

(f) **Feedback and usage counts.** People may give feedback on the scan or a report. It is optional. A feedback record holds the type of scan, the date, where it was asked and the feedback itself. It holds an email address in two cases only: a signed-in person's feedback on their own scan, and an owner's, admin's or analyst's feedback on the Organization's report. Feedback from a Respondent in the

Organization's scan carries no email address and is never linked to answers. The Organization never sees feedback. Written feedback is encrypted, and each feedback record is deleted 24 months after its date. When a person deletes their account, or their account is closed for inactivity, the email address is cleared and the feedback is kept until then. Once a week the operator receives a digest of the feedback and of daily usage counts. The usage counts are one number per step per day, linked to no person, session or draft.

B.2 The privacy notice describes the processing in B.1(c), B.1(d) and B.1(f) and is the Article 13 information for it.

B.3 Zenshin Kaishi does **not** assert that the answers kept under B.1(c) are anonymous. They are unlinked from the person, but they keep the Organization and the Round. An anonymous set would be outside the GDPR and survive a deletion request. A set that is still personal data is not, and the Organization's instruction under clause 9.4 reaches it.

Annex 1: Description of the processing

Subject matter. Running an innovation–culture scan for the Organization and producing its report.

Duration. From the setup of the first Round until the deletion described in clause 9.

Nature and purpose. Inviting the people the Organization names, with the Organization's note where one is written, and reminding those who have not finished once; letting the buyer invite a colleague to set up the scan; collecting answers; scoring and aggregating them into group results; computing the Organization's scores, weighted by headcount across leaders, managers and employees; detecting patterns across roles; producing the Organization's report; telling the participants who finished that the results are open; telling the people running the scan a week before it closes, and when it has closed; sending partners and customers a letter at close where the Organization asked for it (clause 13.7); checking that invitations stay within the places paid for; and the exceptions in clauses 5.3 to 5.5. Counting invitations for invoicing is Zenshin Kaishi's own purpose (Part B.1(e)).

Categories of data subjects.

- The Organization's leaders, managers and employees who are invited. There may be several leaders. Each answers the Leadership Diagnostic for themselves.
- Where the Organization chooses, its partners and customers who are invited.

- The Organization's Administrators (owner, admin, analyst), including a colleague invited to set up the scan.
- People who were invited and never responded, or said no.

Types of personal data.

Category	What
Invitation data	email address (for a withdrawn invitation that was never accepted, a one-way fingerprint of it instead); the group the person was invited as; access role; when the invitation was sent, accepted, declined or withdrawn; whether the one reminder was sent; who sent the invitation, held only until the reminder has gone or its day has passed; invitations to a colleague to set up the scan
Account data	email address; name where given; role in the Organization; sign-in and activity timestamps; when the person first opened their own report (not shown to the Organization)
Participation data	per role: counts of people accepted, pending, declined, withdrawn, started and finished
Answers	coded answers (scales, choices, rankings) and optional written answers to the questions served to that person's group
Disclosure and consent records	which disclosure a person accepted, on which scan, and when; a person's choice to bring an individual scan into the Round, and any later withdrawal of that choice
Interview notes	where a leader chose interview mode (clause 5.5(c)): the interviewer's notes on what the leader said, and who wrote them
Team lead's share	in a team scan, where the lead chose to share (clause 5.5(d)): the lead's answers and remarks, stored encrypted
The note to the people invited	the note (clause 13.6) and who wrote it
Letters sent at close	which letter was sent to which person for which Round, so each goes only once
Report content	group distributions, scores and detected patterns with no identity; quoted leader answers under 5.4(b), shown under the role "Leadership"; unattributed remarks under 5.5(b)
Declarations	which Administrator answered the works council, benchmarking, testimonial and partners' letter questions for a Round, when, the statement chosen, and the version of its wording

Category	What
Organization settings	the Minimum and when its disclosure was accepted; leader naming and when it was switched on; size band, and where given, industry section and country

Special categories. None is asked for. A Respondent could volunteer special-category information in a written answer without being asked. That possibility does not change this annex: none of the scan's questions asks about health, religion, politics, union membership, ethnicity, sexuality, age or disability, and what a person volunteers is handled like any other written answer (encrypted, Annex 2 section 3).

Not part of this processing. A person taking a scan on their own, without an account, may ask for their resume code by email. Zenshin Kaishi then holds that address for up to 48 hours. That happens only on the individual surface, under Part B. Invited Respondents do not pass through it. When that person signs in while the draft still exists, the draft's answers move into their account and the draft is deleted in the same step. From then on the answers are account data, under the account's retention, not the 48-hour draft rule. Signing in can do this only within 48 hours of the draft being started, because an expired draft can no longer be found.

Annex 2: Technical and organizational measures (security summary)

*This annex can be handed to a buyer on its own. It describes the Service as it runs on the date above. Measures marked **(gated)** are enforced by an automated check that runs before every push and on every pull request, and blocks the change if the property stops holding. The non-traceability checks, the Minimum tests and the draft purge test also run before every deploy, and a failure stops the deploy.*

1. Separating the individual from the organization's view

- Aggregation is one-way. The results store the Organization reads holds the Organization, the Round, a pattern, whether it fired, a severity, a time and a group distribution. It holds no user identifier and no session identifier. **(gated)** The only answer text in it is the remarks and quotes described below, stored encrypted and without any identifier.
- No route open to an organization role reads a named person's answers, with two exceptions, each opened by the person concerned: interview mode (clause 5.5(c)), limited to a leader's scan, only while it is open, and only if that leader switched it on;

and a team lead's shared answers (clause 5.5(d)), read from the copy the lead chose to share, never from the answers themselves. The check fails if any other such read appears, and it inspects the interview route query by query. **(gated)**
Interview notes never reach the organization's report. **(gated)**

- Written answers are left out of every organizational aggregate by a default–deny list: a new answer format is excluded unless someone deliberately adds it. **(gated)**
Two exceptions pass through their own gates, not this list. Employees' remarks (clause 5.5(b)) reach the owners, admins and analysts without names, only with the writer's recorded consent, and only at or above the Minimum. Leaders' quotes (clause 5.4(b)) reach the Organization under the role "Leadership", only with that leader's recorded acceptance. Partner and customer written answers never reach the Organization.

2. The Minimum, and who it covers

What	Shown from	Who decides, and what the person is shown
Employee results	5 by default	Nobody needs to choose this. A group below the Minimum is not shown on its own, but its answers count in the Organization's scores. No count is shown from which its size could be worked out
Employee results, lowered	as low as 3 , never lower, and only in scans of up to 20 people, measured as the largest of declared participants, places bought and people invited	The Organization, by accepting a disclosure in the same action. Each employee affected must acknowledge it on their own scan before question one, or cannot answer
Unattributed employee remarks	the employee Minimum, applied to the number of employees who wrote one	The Respondent: declining the disclosure means the question is not asked
Leaders and managers: Leadership Diagnostic, Management Scan, and items asked only of team leaders	1, per role	Fixed by design. They are told in their invitation that their answers can show even when they are the only one in their role
A leader's or manager's answers about their own working life	5, cannot be lowered	Nobody can lower it. These answers are left out of the role's scores

What	Shown from	Who decides, and what the person is shown
Partners and customers	1, as two separate groups	Fixed by design. They are told in their invitation. Never in the culture score; written answers never shown to the Organization
A pattern drawing on several groups	the strictest floor of the groups it uses	Automatic
The Organization's scores	weighted by headcount across leaders, managers and employees	Automatic. An employee group below the Minimum counts, but is not shown on its own
Quoted leader answers	not a floor: attribution, under the role "Leadership", never the name	Each leader, per scan, by accepting a disclosure
A team lead's shared answers	not a floor: the lead's own answers, shared by the lead; the team's side at the Minimum	The lead, after the scan closes

The Organization cannot raise any of these floors above the default. The floor is applied when a result is served, not when it is computed. Lowering the Minimum therefore shows nothing new until the next recalculation.

3. Encryption

- **Answers, unfinished drafts, interview notes, a team lead's shared answers, written feedback, and the quotes and remarks inside stored reports are encrypted at rest** with AES-256-GCM.
- A deployed service without the key **refuses to store an answer** rather than storing it in plain text.
- Other personal data relies on the storage encryption Cloudflare describes for its platform.
- The fingerprint of a withdrawn invitation's address is a keyed one-way hash. Without the key it cannot be recomputed from a list of addresses.
- All traffic uses TLS.

4. Where data is stored

- One database, created with a setting that restricts storage and processing to the European Union, with replication to other regions switched off.
- Requests are handled at the edge location nearest the person. That may be outside the EU if the person is (clause 11.2). Answers and accounts are stored in the EU; Cloudflare's request logs, kept 7 days, fall under clause 11.2.

5. Access roles

Role	Held by	Can see
Respondent	anyone invited, or anyone taking a scan in their own right	their own answers, results and report; their own export; interview notes about them. A leader, manager or employee who has completed their scan in a Round also sees the Organization's report for that Round, with the same floors applied, but not employees' written remarks. In a team scan, a team member who finished also sees the lead's shared answers, once shared
Analyst	assigned by the Organization	the Organization's report, including employees' written remarks, leader quotes and a team lead's shared answers; counts per role; the names, email addresses and roles of the owners, admins and analysts; declarations
Admin, Owner	assigned by the Organization	everything an Analyst sees, plus: inviting people and seeing each invited address and its role; withdrawing invitations; opening and closing Rounds; the settings in clause 5.4; the note to the people invited; making declarations; the Organization's profile. The owner can invite a colleague as admin to set up the scan, and remove them. In interview mode only: the leader's answers and notes while the leader's scan is open
Platform administrator	the operator	the question catalogue, and recording an invoice against a Round (its reference and the number of people paid for), which marks the Round paid. No route gives this role access to answers or to an Organization's people
Operator	the people in clause 4.1	production access through the hosting account

Every Organization-side route checks, on the server, both the role and that the Organization in the request is the caller's own.

6. Sign-in and credentials

- Sign-in is a one-time code, issued and sent by the studio's verification service. No passwords exist.
- One exception: the first use of an invitation, for an address that has no account. Pressing Start on the invitation creates the account, signs the person in from the link, and sends a confirmation email to the invited address. This is refused for an address that already has an account, after the invitation's first use, and for a request from any other site.
- Opening an invitation link changes nothing. Every change is a button press.
- The session cookie is HttpOnly, Secure and SameSite=Lax, valid for 30 days. The origin of the request is checked as a second layer.
- Invitation tokens and resume codes are stored only as SHA-256 hashes. The plain value is sent once and never stored. A resume code carries 256 bits of randomness.
- An invitation link carries its token after the # in the address. Browsers never send that part to a server, so the token does not reach server logs or Referer headers.
- An invitation link works until the Round it was sent for closes. The one reminder, sent five days after the invitation to people who have not finished, carries a second link. Its token is also stored only as a hash.
- After a person deletes their account, sessions issued before the deletion cannot recreate it. The marker that enforces this holds only a hash of the person's sign-in identifier, and is deleted after 30 days.

7. Jobs that run by themselves

Job	Runs	Does
Draft purge	hourly	Deletes every unfinished anonymous draft 48 hours after it was started . Activity on a draft does not extend it. Deletion happens at the first hourly run after expiry. A draft whose owner signs in before then is moved into the account and deleted at once, and the account's retention applies from then on

Job	Runs	Does
Dormancy	hourly	After 24 months without activity, writes to the account holder (or, for an account the Organization manages, its Administrator). Signing in within 30 days keeps the account. Otherwise, after 30 days, closes it as clause 9.2 describes: deletes identity, consent and disclosure records, interview notes, invitation records, shared team-lead answers and the person's note to the people invited; clears the email address from feedback; deletes written answers; keeps coded answers unlinked from the person unless the Organization declined benchmarking; clears payment identifiers from kept rows
Close on date	hourly	Closes Rounds whose closing date has passed, and Rounds open for three months, and recalculates their results. Then sends each participant who finished, and can read the results, one letter that the results are open, and, where the Organization asked (clause 13.7), one letter to each partner and customer who finished. Writes once to the Organization's owners and admins seven days before a Round's closing day, and once when it closes a Round, except to one who already got the letter that the results are open
Invitation reminder	hourly	Sends one reminder, five days after the invitation, to each invited person who has not finished and has not said no, while the Round is open. Clears the record of who sent an invitation once its reminder has gone or its day has passed
Erasure-marker purge	hourly	Deletes deletion markers older than 30 days
Invitation purge	hourly	Deletes invitations that never became an account (never accepted, declined, or withdrawn, fingerprints included) once their Round has been closed for 24 months. First records how many people were invited to each Round affected, so its size does not change
Feedback purge	hourly	Deletes feedback records more than 24 months after their date
Declaration purge	hourly	Deletes the records of the Organization's declarations five years after their Round closed (clause 9.5(a)). Where the Organization declined benchmarking, first notes that on the Round, without any name, so clause 9.2 still applies. Then deletes the account row of a person whose account was already closed and was kept only because a deleted record named it
Feedback digest	weekly	Sends the operator the past week's feedback and usage counts. It reads no email address

8. Deletion and export

- A signed-in person can **export** everything linked to their account, with their answers and interview notes decrypted. They can also **delete** their account. Deletion does what clause 9.2 describes, reports what was deleted, what was unlinked, what was kept and why, and shows the limits in clause 7.4.
- Four things survive deletion: the person's coded answers, unlinked (unless the Organization declined benchmarking); the record of a declaration the person made for an Organization, together with the account row that record names; group results already published; and the person's feedback, with their email address cleared.
- An individual scan that was brought into a Round is treated like the person's other scans: both are unlinked, or both deleted where the Organization declined benchmarking.
- Deletion reaches a withdrawn invitation that holds only the fingerprint of the person's address.

9. Email

- Email to Respondents is sent through the hosting platform's own email binding: invitations, with the Organization's note where one is written; the one reminder; the confirmation after Start; resume codes; inactivity letters; purchase confirmations; the letter that the results are open; the letters to the Organization's owners and admins a week before a Round closes and when it has closed; the letter to partners and customers where the Organization asked for it; and invitations to a colleague to set up the scan. No other provider sends the Service's email.
- A reply to an invitation, its reminder or the confirmation after Start goes to the person who sent the invitation, where the Service still holds their address.
- Sign-in codes are the exception: the studio's verification service sends them, and the Service only relays the request. That service receives the email address and the IP address of the device asking for a code.
- The sending code does not log recipient addresses, resume codes or invitation tokens.
- A second binding can send to one fixed inbox only, enquiry@zenshinkaishi.com. It carries the contact form and the feedback digest. The contact form stores nothing in the Service.
- Mail sent to privacy@, enquiry@ and individualscansupport@zenshinkaishi.com is received in a Microsoft 365 mailbox, outside the hosting platform (Annex 3).

10. Minimisation

- A scan can be started without an account or any identifier.
- No analytics or advertising cookies, and no trackers. Two strictly necessary cookies, both for sign-in.
- The website loads one script that Zenshin Kaishi did not write: Cloudflare Web Analytics, which counts visits. Cloudflare describes it as setting no cookies and not identifying visitors. Zenshin Kaishi relies on that description, as the privacy notice does.
- No AI model reads answers to interpret or score them.
- The note to the people invited is stored as plain text: links and markup are removed when it is saved, and it is cut to 300 characters.

11. Abuse limits

- The contact form and the feedback routes that need no sign-in are limited per visitor IP address. The hosting platform counts the requests. The Service does not store the address.
- Saying no to an invitation needs the invitation's own link, and the answer is the same whatever the link finds.

12. Logging

- Platform logs are switched on so errors can be investigated afterwards. The code logs internal identifiers and error messages, not answers, recipient addresses or credentials. The platform keeps these logs for 7 days, and then deletes them.

13. Verification

- The properties marked **(gated)** are checked before every push and on every pull request, and a failure blocks the push or the merge. The non-traceability checks, the Minimum tests and the draft purge test run again before every deploy, and a failure stops the deploy.
- Each statement in this annex was checked against the running code for this version of the Agreement. The record of those checks is available to the Organization on request.

Annex 3: Sub-processors, and the payment provider

Sub-processors under Part A

Sub-processor	Established	Purpose	Data	Transfer mechanism
Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA	United States, with EU infrastructure	Hosting and running the Service; the database; sending the Service's email through its own email binding; counting requests for the abuse limits; counting visits to the website. Sign-in codes are sent by the studio verification service (below), which also runs on Cloudflare	All personal data in Annex 1	Cloudflare's processing agreement and the EU–US Data Privacy Framework, with Standard Contractual Clauses as fallback (clause 11.3). Storage restricted to the EU (clause 11.1)
Microsoft 365: Microsoft Ireland Operations Ltd, for business customers in the EU	Ireland; the tenant's data location is the European Union (EU/EFTA)	The mailbox for privacy@ , enquiry@ and individualscansupport@zenshinkaishi.com . It receives the contact form's messages and the weekly feedback digest (Annex 2 section 9), and anything a Respondent or the Organization writes to those addresses	What people write to us, and the feedback digest's free text	Microsoft Products and Services Data Protection Addendum; mailbox data stored in the EU/EFTA under the tenant's data location

No other provider sends the Service's email, and no advertising or AI provider processes personal data for the Service.

The sign-in code service. Sign-in codes are issued and checked by a verification service that the studio runs for all its products, on the same Cloudflare account and under the same legal entity. It is not a separate sub-processor. It sees the email

address the code is sent to and the IP address of the device that asked for it, forwarded so its rate limit applies to the visitor. What it stores, and for how long:

- **The email address**, with a hash of the code (never the code itself), the time it was sent and a count of attempts. Deleted when the code is used, after too many wrong attempts, or when the code expires after 10 minutes, whichever comes first.
- **The times codes were sent to that address**, filed under a keyed hash of the address, not the address. Kept 24 hours, to enforce a daily limit per address.
- **A marker that a code was used**, kept 15 minutes so it cannot be used twice.
- **The IP address is never stored**. A keyed hash of it holds the times of requests from that device for one hour, to enforce an hourly limit.
- **Its logs** carry short fragments of those hashes, never the address, the IP address or the code, and are kept for 7 days like the Service's own (Annex 2 section 12).

Its storage is not restricted to the European Union, unlike the Service's database (clause 11.1). Everything in it is gone within 24 hours.

Stripe: the payment provider, and why it is not listed above

Stripe (Stripe Payments Europe, Limited, Ireland, the Stripe entity for an account in the Netherlands) processes payments for Zenshin Kaishi (Part B.1(e)). It is its own controller for fraud prevention and its legal duties. It is not a sub-processor of the Organization's scan. The public sub-processor page names it all the same, so that a person who pays knows who takes the payment. What it touches depends on who is buying:

An Organization buying a Round. Stripe receives the purchasing Administrator's email address (as the receipt address), the billing name and address (required), a VAT number if one is given, payment details, and this information in the payment record: the number of people to be invited, Zenshin Kaishi's internal identifier for the purchasing account, whether the scan is a team scan, whether the buyer added the scan to the Organization they already belong to (with that Organization's internal identifier) or started a separate one, which version of Zenshin Kaishi's terms of service was accepted and when, and, for a repeat, the internal identifier of the earlier Round of the same kind. **Stripe receives no Respondent's name, email address, invitation or answer, and no report content.** A Round bought by quote is invoiced through Stripe, and the invoice carries the Round's identifier and the number of people invited. For a top-up, an Administrator adds places online to a Round already paid for. Stripe then receives the same billing details, the Round's identifier, the number of places added and already bought, the buying Administrator's internal identifier, which version of the

terms of service was accepted and when, and, where the Round is a repeat, the identifier of the earlier Round.

An individual buying their own scan. Stripe receives the buyer's account email (as the receipt address), payment details, the billing country or address where needed to calculate VAT, and Zenshin Kaishi's internal identifier for the scan being paid for, when the buyer ticked the withdrawal box and which wording it carried, and which version of the terms of service was accepted and when. **It receives no answers and no results.**

The one place the two meet. When a person who paid for their own scan brings it into their Organization's Round, the payment is refunded automatically. The refund record sent to Stripe carries only the reference of the person's own paid scan. It carries no answers, no Organization name and no email address. When that person's account later closes, the payment and refund identifiers are cleared from the kept scan.

Signatures

For Plakboom B.V. (Zenshin Kaishi)

Name: _____

Title: _____

Date: _____

Signature: _____

For the Organization

Organization: _____

Name: _____

Title: _____

Date: _____

Signature: _____